受験番号		氏名	

令和５年度神戸大学「志」特別選抜
最終選抜（工学部情報知能工学科）

令和４年１１月５日 実施

試験問題「総合問題（情報知能工学）」

全５ページ（表紙を除く）

注意事項：

1. 試験中は、試験監督の指示に従うこと。
   従わない場合は、不正行為と見なすことがあります。
2. 解答開始の合図があるまで、試験問題を開かないこと。
3. 「受験者心得」で持ち込みが認められたもの以外は、机の上に置かず、カバンの中にしまうこと。
   試験時間中に使用を認められていない物品を机の上に置いたり、使用したりした場合は、不正行為とみなすことがあります。
4. 時計のアラーム、時報、目覚まし音の設定をしている人は解除してください。
5. 携帯電話・スマートフォン等の電子機器類を時計として使用することはできません。これらを持っている場合は、アラームを設定している人は解除し、必ず電源を切ってから、カバンの中にしまうこと。
   アラームの解除の仕方が分からない場合は、監督者に申し出ること。
   試験時間中に、これらを身に着けていた場合は、不正行為と見なすことがあります。
6. カバンなどの持ち物は、椅子の下に置くこと。
7. 机の下の物入れは、使用しないこと。
8. 答案は、黒鉛筆またはシャープペンシルで解答すること。
9. 答案は、別紙の解答用紙に解答すること。（大問ごとに、解答用紙が分かれています）
10. 試験時間中に質問等がある場合は、手を挙げて試験監督に申し出ること。
11. 試験途中の退室は認めません。
    ただし、トイレに行きたい場合や気分が悪くなった場合は、手を挙げて試験監督に申し出てください。
12. 解答開始の合図の後、まず、問題・解答・下書き用紙全てに、受験番号、氏名を記入すること。
13. 配布した用紙（問題・解答・下書き用紙）は、試験時間終了後にすべて回収します。持ち帰ることはできないので、注意すること。

【問題 1】

自然数 a に対して m を $10^{m-1} \leqq a < 10^m$ を満たす自然数とする。$0 \leqq a_i \leqq 9$ を満たす整数 a_i $(i = 1, \cdots, m)$ によって $a = \sum_{i=1}^{m} a_i 10^{i-1}$ と表されるとき，$h(a) = \sum_{i=1}^{m} (a_i)^2$ と定める。例えば，$153 = 3 \times 10^0 + 5 \times 10^1 + 1 \times 10^2$ と表せるので，$h(153) = 3^2 + 5^2 + 1^2 = 35$ である。数列 $\{b_n\}$ が次の漸化式を満たすとき，$\{b_n\}$ を自然数 a から始まる h 列であるという。

$$\begin{cases} b_1 &= a \\ b_{n+1} &= h(b_n) \end{cases}$$

次の問 1 から問 7 に答えなさい。

問 1. $h(299)$ と $h(3281)$ の値を求めなさい。

問 2. 356 から始まる h 列 $\{b_n\}$ について，b_5 の値を求めなさい。

問 3. 自然数 a と m について $10^{m-1} \leqq a < 10^m$ が成り立つとき，$h(a) \leqq 81m$ であることを示しなさい。

問 4. 4 以上の自然数 m について，$81m < 10^{m-1}$ であることを示しなさい。

問 5. a を 1000 以上の自然数とする。$h(a) < a$ であることを示しなさい。

問 6. a を自然数とする。a から始まる h 列 $\{b_n\}$ がいずれ循環すること，すなわち，$n_1 < n_2$ かつ $b_{n_1} = b_{n_2}$ となる自然数 n_1，n_2 が存在することを示しなさい。

問 7. k を 2 以上の自然数とする。自然数 a を上述のように $a = \sum_{i=1}^{m} a_i 10^{i-1}$ と表すとき，$h_k(a) = \sum_{i=1}^{m} (a_i)^k$ と定める。つまり，関数 h_2 は h に他ならない。関数 h_k について気がついたことを述べなさい。

【問題 2】

次の問 1 から問 3 に答えなさい。

問 1. ニュートンの運動の第二法則「物体の運動量の変化は，物体に作用する力積に比例し，方向が同じになる」を図や式を用いて説明しなさい。

問 2. ニュートンの運動の第二法則を用いて，密度（単位体積あたりの質量）ρ，流速 V で一様かつ水平に流れる流体中に置かれた平らな板に作用する力を，ニュートンが実際に示した考え方に沿って求めてみよう。ただし，図 2-1 のように板は流れに対して角度 θ で置かれており，板の面積は A，奥行きは 1 とする。

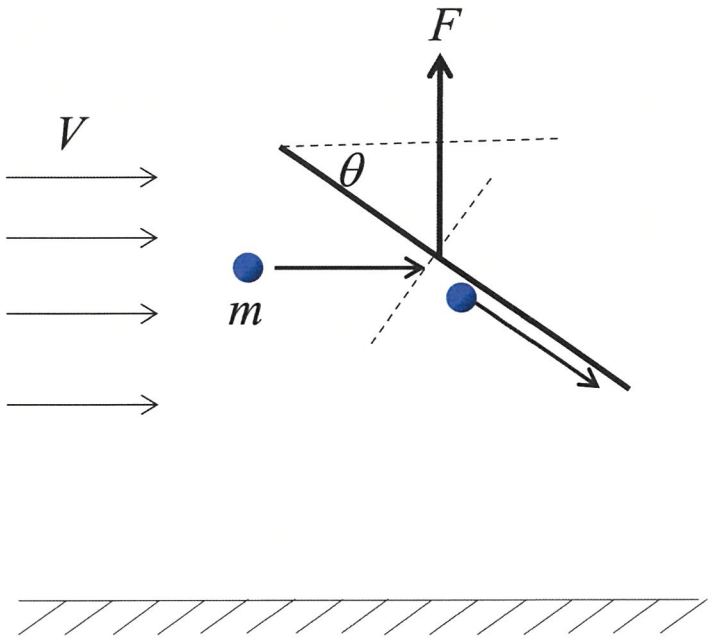

図 2-1

(1) ここでは流体は，互いに影響を及ぼさない質量 m の粒子（質点）が，単位体積当たり均一に N 個集まって構成されているとする。流体の密度 ρ を m と N を用いて表しなさい。

(2) 粒子は板に衝突する前は速度 V で水平に運動している。板に衝突後は図 2-1 のように方向を変えて板に沿って速度 V で運動するとする。このとき，ニュートンの運動の第三法則を用いて，一つの粒子の衝突によって板に作用する地面に対して垂直方向の力積を求めなさい。

(3) 質点が自由に通過できる仮想的な面積 1 の面を流れに垂直に置くとき，単位時間にこの面を通過する粒子の個数を求めなさい。

(4) 単位時間に板に衝突する粒子の個数を求めなさい。

(5) (2) と (4) の結果より，密度 ρ の流体中に置かれた板に作用する地面に垂直方向の力 F を求めなさい。

次ページに続く

問3. ニュートンが求めたこの答え F は，特に θ が小さい場合，実際の流体に置かれた場合と比較して過小評価する結果となる。水平に流れる流体中に置かれた板の周りの流れを可視化した写真（図2-2）を参考に，問2で示したニュートンの考え方のどの部分に，実際の流れとの相違があったのかを考察しなさい。

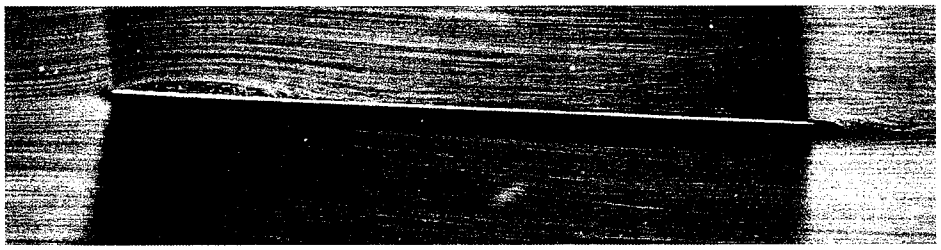

図 2-2

【問題 3】

高度情報社会においては暗号化技術は必要不可欠となっている。情報の暗号化は古くから行われており，古典的な暗号技術としては，情報を伝達する二者間で定めたルール（鍵）に従って，文字を別の文字で置き換える換字式暗号や，文字の順序を並べ替える転置式暗号が用いられてきた。この鍵が第三者に知られると情報が漏れてしまう。また，時間をかければ試行錯誤によって鍵を推定されることがある。

このような，暗号化と復号に共通の鍵が用いられる暗号化方式は，共通鍵暗号と呼ばれる。現代の共通鍵暗号方式はより複雑であり，鍵が漏洩しなければ実時間で解読することは不可能とされている。しかし，ここで問題となるのは二者間での鍵の共有である。

図 3-1 は，鍵付きの鞄を例に共通鍵暗号の考え方を示している。鍵付きの鞄に文章を入れて相手に送る場合，その鍵も何らかの方法で相手に渡さなければならない。鍵が盗まれると鞄が開けられてしまう恐れがあるため，鍵を安全に相手に渡すことが重要となる。この「鍵の配送問題」は古典暗号の時代から長年の課題であり，多くの暗号は鍵の漏洩によって解読されてきた。

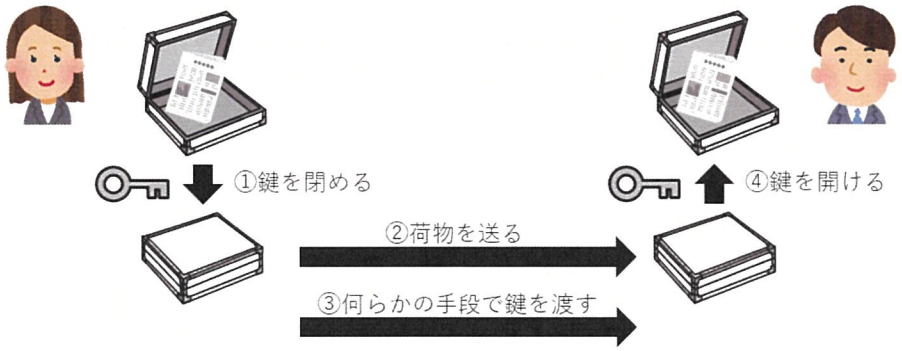

図 3-1：鍵付きの鞄の例

これに対して 1970 年代に提案された公開鍵暗号は，暗号化に用いる鍵（公開鍵）と復号に用いる鍵（秘密鍵）を分離するというアイデアによって鍵の配送問題を解決している。公開鍵と秘密鍵は，公開鍵で暗号化した情報は秘密鍵でしか復号できないという特性を持った鍵のペアである。

次の問 1 から問 4 に答えなさい。

問 1. 日常の中で暗号技術が使われている具体例を 2 つ示しなさい。

問 2. 古典的な暗号が解読される可能性として，鍵の漏洩以外に，どのような原因が考えられるか述べなさい。

問 3. 公開鍵と秘密鍵は南京錠で例えることができる。開いている南京錠を閉めることは誰でもできるが，鍵を持っている者しか南京錠を開けることはできない。図 3-1 では鍵付きの鞄を使って文章を送る例を示したが，同様に「南京錠」,「南京錠を開ける鍵」,「南京錠で閉じられる鞄」を使って送信者から受信者に文章を送る方法を述べなさい。

次ページに続く

問 4. 共通鍵暗号方式の一つは，大きな数の素因数分解が困難であることを利用して，次の事実に基づいて，公開鍵と秘密鍵のペアを生成する。

ここで，p と q を異なる素数とし，$n = pq$ とする。L を $p-1$ と $q-1$ の最小公倍数とし，L と互いに素な自然数 e を選ぶ。e と d の積を L で割った余りが 1 となる自然数 d は容易に求められる。このとき，n より小さい自然数 x に対して，x^e を n で割った余りを y とすると，y^d を n で割った余りが x となることが知られている。

例えば，$p = 2$，$q = 11$ とすれば，$n = 22$，$L = 10$ となる。ここで，$e = 7$ と選ぶと，$d = 3$ と求められる。$x = 4$ のとき，$x^e = 16384$ となり $y = 16$ となる。また，$y^d = 4096$ であり，これを n で割った余りは 4 となり x と等しくなる。

このとき，x を暗号化したものが y と考えることができる。

p，q，n，e，d のうち，公開鍵として使用されるものを全て示しなさい。また,「素因数分解」という語を用いて，その理由を述べなさい。